Exhibit 300: Part I: Summary Information and Justification (All Capital Assets)

I.A. Overview

1. Date of Submission:	8/4/2006
2. Agency:	Department of State
3. Bureau:	Information Resource Management
4. Name of this Capital Asset:	Global Network
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.)	014-00-02-00-01-1100-00
6. What kind of investment will this be in FY2008? (Please NOTE: Investments moving to O&M ONLY in FY2008, with Planning/Acquisition activities prior to FY2008 should not select O&M. These investments should indicate their current status.)	Mixed Life Cycle
7. What was the first budget year this investment was submitted to OMB?	FY2005

8. Provide a brief summary and justification for this investment, including a brief description of how this closes in part or in whole an identified agency performance gap:

The Global Network Program operates and modernizes the Department of State's global network. The global network forms the backbone of the Department's IT infrastructure, providing essential communication to 260 diplomatic posts around the world, including embassies, consulates, and multi-agency missions. The network also connects 240 additional sites, such as post annexes. Employees increasingly rely on the network's communications to further the United States' foreign policy goals. The Department envisions an IT environment that allows access to IT resources at anytime from anywhere in the world. To support this vision, the Global Network is taking bold steps to provide a network that is secure, always available, and has sufficient bandwidth to support a multitude of services. The Global Network is partnering with the US Agency for International Development (USAID) to explore integrating USAID and State's IT infrastructure. IT integration is a critical step in achieving the joint strategic goal to "ensure a high quality workforce supported by modern and secure infrastructure and operational capabilities," (State and USAID Joint Strategic Plan FY04-09). This effort also helps prepare the Department for the IT Infrastructure Line of Business Initiative. The Global Network is a consolidated business case, integrating six subprograms: 1. Enterprise Network Management (ENM) modernizes and maintains communications over the global network, providing essential connectivity to Foreign Affairs personnel around the world. 2. Bandwidth Management analyzes network capacity requirements, helps posts procure network connectivity, and provides funding for global bandwidth. Use of innovative technologies has helped the program increase bandwidth capacity while reducing the cost per bit of bandwidth. 3. Enterprise Software Licensing establishes and maintains enterprise software licensing agreements, lowering the prices the Department pays per license based on volume purchases. 4. The Alternate Communications Site (ACS), housed at a FEMA location, is an alternate site for routing essential communications in the event the primary locations are not operational. 5. The InfoCenter is a 24-hour IT help desk that provides first-tier customer support for embassies, consulates, and offices throughout the world. 6. In-Line Network Encryption secures the Department's command and control telegraphic network by encrypting all National Security communications.

9. Did the Agency's Executive/Investment Committee approve this request?	Yes
a. If "yes," what was the date of this approval?	8/4/2006
10. Did the Project Manager review this Exhibit?	Yes
12. Has the agency developed and/or promoted cost effective, energy efficient and environmentally sustainable techniques or practices for this project.	Yes
a. Will this investment include electronic assets (including	Yes

computers)?	
b. Is this investment for new construction or major retrofit of a Federal building or facility? (answer applicable to non-IT assets only)	No
1. If "yes," is an ESPC or UESC being used to help fund this investment?	
2. If "yes," will this investment meet sustainable design principles?	
3. If "yes," is it designed to be 30% more energy efficient than relevant code?	
13. Does this investment support one of the PMA initiatives?	Yes
If "yes," check all that apply:	Expanded E-Government, Right Sized Overseas Presence
13a. Briefly describe how this asset directly supports the identified initiative(s)?	The Global Network investment supports the PMA's goal of Rightsized Overseas Presence by: Providing and deploying the infrastructure for an integrated system of networks with other agencies that have an overseas presence; Centralizing logistics and financial applications so that information is shared more quickly; Providing an easy single-point-of-contact access to licensing services to reduce internal costs; and Enabling remote management of IT functions to domestic locations.
14. Does this investment support a program assessed using the Program Assessment Rating Tool (PART)? (For more information about the PART, visit www.whitehouse.gov/omb/part.)	No
a. If "yes," does this investment address a weakness found during the PART review?	No
b. If "yes," what is the name of the PART program assessed by OMB's Program Assessment Rating Tool?	
c. If "yes," what PART rating did it receive?	
15. Is this investment for information technology?	Yes
If the answer to Question: "Is this investment for information technology?" was "Yes," complete this sub-section. If the answer is "No," do not answer this sub-section.	
For information technology investments only:	
16. What is the level of the IT Project? (per CIO Council PM Guidance)	Level 2
17. What project management qualifications does the Project Manager have? (per CIO Council PM Guidance):	(1) Project manager has been validated as qualified for this investment
18. Is this investment identified as "high risk" on the Q4 - FY 2006 agency high risk report (per OMB's "high risk" memo)?	No
19. Is this a financial management system?	No
a. If "yes," does this investment address a FFMIA compliance area?	No
1. If "yes," which compliance area:	
2. If "no," what does it address?	
b. If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update	

required by Circular A-11 section 52	
20. What is the percentage breakout for the total FY2008 funding request for the following? (This should total 100%)	
Hardware	60
Software	21
Services	19
Other	0
21. If this project produces information dissemination products for the public, are these products published to the Internet in conformance with OMB Memorandum 05-04 and included in your agency inventory, schedules and priorities?	N/A
23. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval?	Yes

I.D. Performance Information

In order to successfully address this area of the exhibit 300, performance goals must be provided for the agency and be linked to the annual performance plan. The investment must discuss the agency's mission and strategic goals, and performance measures must be provided. These goals need to map to the gap in the agency's strategic goals and objectives this investment is designed to fill. They are the internal and external performance benefits this investment is expected to deliver to the agency (e.g., improve efficiency by 60 percent, increase citizen participation by 300 percent a year to achieve an overall citizen participation rate of 75 percent by FY 2xxx, etc.). The goals must be clearly measurable investment outcomes, and if applicable, investment outputs. They do not include the completion date of the module, milestones, or investment, or general goals, such as, significant, better, improved that do not have a quantitative or qualitative measure.

Agencies must use Table 1 below for reporting performance goals and measures for all non-IT investments and for existing IT investments that were initiated prior to FY 2005. The table can be extended to include measures for years beyond FY 2006.

Performance Information Table 1:

Fiscal Year	Strategic Goal(s) Supported	Performance Measure	Actual/baseline (from Previous Year)	Planned Performance Metric (Target)	Performance Metric Results (Actual)
2005	Per FY 2005 OMB A-11 guidance, new investments initiated in FY 2005 are not required to report in Table 1.	N/A	N/A	N/A	N/A

All new IT investments initiated for FY 2005 and beyond must use Table 2 and are required to use the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM). Please use Table 2 and the PRM to identify the performance information pertaining to this major IT investment. Map all Measurement Indicators to the corresponding "Measurement Area" and "Measurement Grouping" identified in the PRM.

There should be at least one Measurement Indicator for at least four different Measurement Areas (for each fiscal year). The PRM is available at www.egov.gov.

Performance Information Table 2:

Fiscal Year	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Planned Improvement to the Baseline	Actual Results
2005	Customer Results	Service Accessibility	Integration	Percent of enterprise standardized under Central Enterprise Oversight.	Baseline is 0% in FY2004.	Increase to 10% of domestic sites and foreign posts in FY2005.	As of September 30, 2005, 10% of domestic and foreign posts are standardized under Central Enterprise Oversight.
2005	Mission and Business Results	Information and Technology Management	IT Infrastructure Maintenance	Cost per bit of bandwidth decreases due to network modernization.	Baseline is $.45/bit in FY2004.	Decrease cost per bit of bandwidth to $.40/bit in FY2005 - for a 10% annual decrease.	As of September 30, 2005, the cost per bit has decreased to $.40/bit.
2005	Processes and Activities	Security and Privacy	Security	Percent of enterprise covered by real-time patch management and security monitoring tools.	Baseline is 0% in FY2004.	Increase to 10% of targeted devices in FY2005.	As of September 30, 2005, 10% of targeted devices are covered by real-time patch management and security monitoring tools.
2005	Technology	Reliability and Availability	Availability	Percent of network availability. Number of official diplomatic posts installed with VPN alternative routes.	Baseline is 99% availability in FY2004 and 200 VPN alternative routes installed to official enterprise sites.	Increase network availability to 99.5% and complete 260 VPN alternative routes to all official enterprise, diplomatic posts, such as embassies, consulates and missions in FY2005.	As of September 30, 2005, network availability is 99.5% and 260 official diplomatic posts have been installed with VPNs.
2006	Customer Results	Service Accessibility	Integration	Percent of enterprise standardized under Central Enterprise Oversight.	Baseline is 0% in FY2004.	Increase to 20% of domestic sites and foreign posts in FY2006.	As of August 31, 2006, 20% of domestic and foreign posts are standardized under Central Enterprise Oversight.
2006	Mission and Business Results	Information and Technology Management	IT Infrastructure Maintenance	Cost per bit of bandwidth decreases due to network modernization.	Baseline is $.45/bit in FY2004.	Decrease cost per bit of bandwidth to $.36/bit in FY 2006 - for a 10% annual decrease.	As of August 31, 2006, the cost per bit has decreased to $.36/bit.
2006	Processes and Activities	Security and Privacy	Security	Percent of enterprise covered by real-time patch management and security monitoring tools.	Baseline is 0% in FY2004.	Increase to 30% of targeted devices in FY2006.	As of August 31, 2006, 30% of targeted devices are covered by real-time patch management and security monitoring tools.
2006	Technology	Reliability and Availability	Availability	Percent of network availability. Number of sites installed with VPNs.	Baseline is 99% availability in FY2004 and 200 VPNs installed.	Increase network availability to 99.6% in FY2006. Install 40 additional VPNs(for a total of 300 VPNs) to formerly convenience sites reclassified to enterprise sites such as post annexes and other sites with official consular staff.	As of August 31, 2006, network availability is 99.6%. 2 additional official diplomatic posts have been installed with VPNs and 38 post annex sites have been installed with VPNs for a total of 300 VPNs in place.
2007	Customer Results	Service Accessibility	Integration	Percent of enterprise standardized under Central Enterprise Oversight.	Baseline is 0% in FY2004.	Increase to 30% of domestic sites and foreign posts in FY2007.	TBD

2007	Mission and Business Results	Information and Technology Management	IT Infrastructure Maintenance	Cost per bit of bandwidth decreases due to network modernization.	Baseline is $.45/bit in FY2004.	Decrease cost per bit of bandwidth to $.32/bit in FY2007 - for a 10% annual decrease.	TBD
2007	Processes and Activities	Security and Privacy	Security	Percent of enterprise covered by real-time patch management and security monitoring tools.	Baseline is 0% in FY2004.	Increase to 50% of targeted devices in FY2007.	TBD
2007	Technology	Reliability and Availability	Availability	Percent of network availability. Number of sites installed with VPNs.	Baseline is 99% availability in FY2004 and 200 VPN alternative routes installed.	Increase network availability to 99.7% in FY2007. Install 40 additional VPNs(for a total of 340 VPNs) to formerly convenience sites reclassified to enterprise sites such as post annexes and other sites with official consular staff.	TBD
2008	Customer Results	Service Accessibility	Integration	Percent of enterprise standardized under Central Enterprise Oversight.	Baseline is 0% in FY2004.	Increase to 40% of domestic sites and foreign posts in FY2008.	TBD
2008	Mission and Business Results	Information and Technology Management	IT Infrastructure Maintenance	Cost per bit of bandwidth decreases due to network modernization.	Baseline is $.45/bit in FY2004.	Decrease cost per bit of bandwidth to $.29/bit in FY2008 - for a 10% annual decrease.	TBD
2008	Processes and Activities	Security and Privacy	Security	Percent of enterprise covered by real-time patch management and security monitoring tools.	Baseline is 0% in FY2004.	Increase to 70% of targeted devices in FY2008	TBD
2008	Technology	Reliability and Availability	Availability	Percent of network availability. Number of sites installed with VPNs.	Baseline is 99% availability in FY2004 and 200 VPNs installed.	Maintain network availability at 99.7% in FY2008. Install 40 additional VPNs(for a total of 380 VPNs) to formerly convenience sites reclassified to enterprise sites such as post annexes and other sites with official consular staff.	TBD

I.E. Security and Privacy

In order to successfully address this area of the business case, each question below must be answered at the system/application level, not at a program or agency level. Systems supporting this investment on the planning and operational systems security tables should match the systems on the privacy table below. Systems on the Operational Security Table must be included on your agency FISMA system inventory and should be easily referenced in the inventory (i.e., should use the same name or identifier).

All systems supporting and/or part of this investment should be included in the tables below, inclusive of both agency owned systems and contractor systems. For IT investments under development, security and privacy planning must proceed in parallel with the development of the system/s to ensure IT security and privacy requirements and costs are identified and incorporated into the overall lifecycle of the

system/s.	
Please respond to the questions below and verify the system owner took the following actions:	
1. Have the IT security costs for the system(s) been identified and integrated into the overall costs of the investment:	Yes
a. If "yes," provide the "Percentage IT Security" for the budget year:	5
2. Is identifying and assessing security and privacy risks a part of the overall risk management effort for each system supporting or part of this investment.	Yes
5. Have any weaknesses related to any of the systems part of or supporting this investment been identified by the agency or IG?	Yes
a. If "yes," have those weaknesses been incorporated agency's plan of action and milestone process?	Yes
6. Indicate whether an increase in IT security funding is requested to remediate IT security weaknesses?	No
a. If "yes," specify the amount, provide a general description of the weakness, and explain how the funding request will remediate the weakness.	

8. Planning & Operational Systems - Privacy Table:

Name of System	Is this a new system?	Is there a Privacy Impact Assessment (PIA) that covers this system?	Is the PIA available to the public?	Is a System of Records Notice (SORN) required for this system?	Was a new or amended SORN published in FY 06?
Application Manager	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Application Manager for ClassNet	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
ClassNet Transport GSS	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
IEMS for ClassNet (IEMS-C)	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Integrated Enterprise Management System (IEMS)	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
iPost	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
iPost for ClassNet (iPost-C)	Yes	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
NetVCR	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.

OpenNet Transport GSS	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Security Manager	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Security Manager for ClassNet	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
System Management Server (SMS)	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
System Management Server (SMS) for ClassNet (SMS-C)	Yes	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Universal Trouble Ticket	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Windows/Active Directory	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Windows/Active Directory for ClassNet	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.

I.F. Enterprise Architecture (EA)

In order to successfully address this area of the business case and capital asset plan you must ensure the investment is included in the agency's EA and Capital Planning and Investment Control (CPIC) process, and is mapped to and supports the FEA. You must also ensure the business case demonstrates the relationship between the investment and the business, performance, data, services, application, and technology layers of the agency's EA.

1. Is this investment included in your agency's target enterprise architecture?	Yes
a. If "no," please explain why?	
2. Is this investment included in the agency's EA Transition Strategy?	Yes
a. If "yes," provide the investment name as identified in the Transition Strategy provided in the agency's most recent annual EA Assessment.	Global Network
b. If "no," please explain why?	

3. Service Reference Model (SRM) Table:	

Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.whitehouse.gov/omb/egov/.

Agency Component Name	Agency Component Description	Service Domain	FEA SRM Service Type	FEA SRM Component	FEA Service Component Reused Name	FEA Service Component Reused UPI	Internal or External Reuse?	BY Funding Percentage
Configuration Management	Defines the set of capabilities that control the hardware and software environments, as well as documents of an organization.	Business Management Services	Management of Processes	Configuration Management			No Reuse	1
Program/Project Management	Defines the set of capabilities for the management and control of a particular effort of an organization.	Business Management Services	Management of Processes	Program / Project Management			No Reuse	2
Network Management	Defines the set of capabilities involved in monitoring and maintaining a communications network in order to diagnose problems, gather statistics, and provide general usage.	Business Management Services	Organizational Management	Network Management			No Reuse	1
Assistance Request	Defines the set of capabilities that support the solicitation of support from a customer.	Customer Services	Customer Initiated Assistance	Assistance Request			No Reuse	2
Data Network Services	Executes, maintains, and supports the devices, facilities, and standards that provide the computing and networking within and between enterprises.	Support Services	Communication	NEW			No Reuse	56
Access Control	Defines the set of capabilities that support the management of permissions for logging onto a computer or network.	Support Services	Security Management	Access Control			No Reuse	4
Encryption	Defines the set of capabilities that support the encoding of data for security purposes.	Support Services	Security Management	Cryptography			No Reuse	9
Continuity of Operations	The execution of contingency plans for operations during crisis, unforeseen circumstances, or disruptions in normal day-to-day operations.	Support Services	Security Management	NEW			No Reuse	3
Issue Tracking	Receive and track user-reported issues and problems in using IT systems, including help desk calls.	Support Services	Systems Management	Issue Tracking			No Reuse	1
License Management	Defines the set of capabilities that support the purchase, upgrade, and tracking of legal usage contracts for system software and applications.	Support Services	Systems Management	License Management			No Reuse	16
Remote Systems Control	Defines the set of capabilities that support the monitoring, administration, and usage of applications and enterprise systems from locations outside of the immediate system environment.	Support Services	Systems Management	Remote Systems Control			No Reuse	2
Software	Defines the set of capabilities that support	Support	Systems	Software			No Reuse	2

Distribution	the propagation, installation, and upgrade of written computer programs, applications, and components.	Services	Management	Distribution				
System Resource Monitoring	Defines the set of capabilities that support the balance and allocation of memory, usage, disk space, and performance on computers and their applications.	Support Services	Systems Management	System Resource Monitoring			No Reuse	1

Use existing SRM Components or identify as "NEW". A "NEW" component is one not already identified as a service component in the FEA SRM.

A reused component is one being funded by another investment, but being used by this investment. Rather than answer yes or no, identify the reused service component funded by the other investment and identify the other investment using the Unique Project Identifier (UPI) code from the OMB Ex 300 or Ex 53 submission.

'Internal' reuse is within an agency. For example, one agency within a department is reusing a service component provided by another agency within the same department. 'External' reuse is one agency within a department reusing a service component provided by another agency in another department. A good example of this is an E-Gov initiative service being reused by multiple organizations across the federal government.

Please provide the percentage of the BY requested funding amount used for each service component listed in the table. If external, provide the funding level transferred to another agency to pay for the service.

4. Technical Reference Model (TRM) Table:

To demonstrate how this major IT investment aligns with the FEA Technical Reference Model (TRM), please list the Service Areas, Categories, Standards, and Service Specifications supporting this IT investment.

FEA SRM Component	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard	Service Specification (i.e. vendor or product name)
Issue Tracking	Component Framework	Data Management	Reporting and Analysis	Remedy Action Request System
Access Control	Component Framework	Security	Certificates / Digital Signatures	Digital Certificate Authentication - Patriot Technologies RSA Secure
Access Control	Component Framework	Security	Certificates / Digital Signatures	Secure Sockets Layer (SSL) - Microsoft supported
System Resource Monitoring	Service Access and Delivery	Access Channels	Other Electronic Channels	NetIQ Application Manager
Assistance Request	Service Access and Delivery	Access Channels	Other Electronic Channels	Remedy Action Request System
Network Management	Service Access and Delivery	Delivery Channels	Intranet	Hewlett-Packard OpenView
Access Control	Service Access and Delivery	Service Requirements	Authentication / Single Sign-on	Cisco Access Control System
Access Control	Service Access and Delivery	Service Requirements	Hosting	Microsoft Active Directory
Program / Project Management	Service Access and Delivery	Service Requirements	Legislative / Compliance	Business Engine Microframe Program Manager (MPM)
Program / Project Management	Service Access and Delivery	Service Requirements	Legislative / Compliance	Section 508 (all systems must comply)
Software Distribution	Service Access and Delivery	Service Transport	Service Transport	File Transfer Protocol (FTP) - Microsoft supported
License Management	Service Access and Delivery	Service Transport	Service Transport	Hyper Text Transfer Protocol (HTTP) - Microsoft supported
Network Management	Service Access and Delivery	Service Transport	Service Transport	Internet Protocol (IP) v4 transitioning to v6 - Cisco,

				Microsoft Supported
Network Management	Service Access and Delivery	Service Transport	Service Transport	IP Security (IPSEC) - Cisco, Nortel supported
Network Management	Service Access and Delivery	Service Transport	Service Transport	Taave Software Co. PReView
Network Management	Service Access and Delivery	Service Transport	Service Transport	Transport Control Protocol (TCP) - Cisco, Microsoft supported
Remote Systems Control	Service Platform and Infrastructure	Database / Storage	Database	Microsoft SQL Server
License Management	Service Platform and Infrastructure	Database / Storage	Database	Oracle Enterprise Edition 9i
Software Distribution	Service Platform and Infrastructure	Delivery Servers	Web Servers	Microsoft Internet Information Server
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Local Area Network (LAN)	Ethernet - Cisco supported
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Cisco Routers, including 2621xm, 7208vxr
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Cisco Switches, including 2950, 3750, 6509
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Lucent Optical Switching, OC3, OC12, OC48
Cryptography	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Nortel 600, 1700, 2700; General Dynamics Taclane, Sectera
Remote Systems Control	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Hewlett-Packard Enterprise Server, including DL380
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Wide Area Network (WAN)	Marconi Asynchronous Transfer Mode (ATM) - ServiceOnData
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Wide Area Network (WAN)	Niksun NetVCR
Remote Systems Control	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Microsoft SMS Deployment Management
Configuration Management	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Opsware Network Automation System

Service Components identified in the previous question should be entered in this column. Please enter multiple rows for FEA SRM Components supported by multiple TRM Service Specifications

In the Service Specification field, Agencies should provide information on the specified technical standard or vendor product mapped to the FEA TRM Service Standard, including model or version numbers, as appropriate.

5. Will the application leverage existing components and/or applications across the Government (i.e., FirstGov, Pay.Gov, etc)? Yes

a. If "yes," please describe.

This investment uses GSA's SMARTBUY program to purchase licenses and maintenance for enterprise agreements with Oracle and WinZip. This investment uses the Diplomatic Telecommunication Service (DTS) for backup circuits to our Internet Service Provider (ISP) Virtual Private Network (VPN) primary circuits to 260 embassies and consulates worldwide. These primary and backup circuits enable our highly available network percentage of 99.6% this fiscal year.

6. Does this investment provide the public with access to a government automated information system? No

a. If "yes," does customer access require specific software (e.g., a specific web browser version)?	
1. If "yes," provide the specific product name(s) and version number(s) of the required software and the date when the public will be able to access this investment by any software (i.e. to ensure equitable and timely access of government information and services).	

Exhibit 300: Part II: Planning, Acquisition and Performance Information

II.A. Alternatives Analysis

Part II should be completed only for investments identified as "Planning" or "Full Acquisition," or "Mixed Life-Cycle" investments in response to Question 6 in Part I, Section A above.

In selecting the best capital asset, you should identify and consider at least three viable alternatives, in addition to the current baseline, i.e., the status quo. Use OMB Circular A- 94 for all investments, and the Clinger Cohen Act of 1996 for IT investments, to determine the criteria you should use in your Benefit/Cost Analysis.

1. Did you conduct an alternatives analysis for this project?	Yes
a. If "yes," provide the date the analysis was completed?	5/21/2004
b. If "no," what is the anticipated date this analysis will be completed?	
c. If no analysis is planned, please briefly explain why:	

4. What specific qualitative benefits will be realized?

This study indicates Department-Centralized Management would have favorable effects on all criteria. This alternative would ensure network security, increase network availability, and is the lowest cost alternative. Centralized management would improve communication, support the DoS strategic goals for merging network operations, and standardize processes and desktop configurations. Alternative 1, Department-Centralized Management would also have favorable quantitative benefits. Department-Centralized Management, is the low-cost alternative with a NPV of $752 million. Major factors making this option the low-cost alternative include innovative programs involving the procurement of bandwidth and enterprise software licensing. By installing Virtual Private Network circuits, the Department can significantly reduce its bandwidth costs by approximately $700 million (compared to Alternative 2) over the next ten years, while increasing both network capacity and availability. Cost savings for enterprise software licensing also contribute to Alternative 1 being the low-cost alternative. Department-Centralized Management would help the Department decrease bandwidth costs from $0.37/bit to $0.10/bit by FY2014 and increase network availability to 99.7% by FY2007. Alternative 1's costs were comparable to the baseline, but Alternative 1 would achieve many efficiencies through centralized management that the status quo could not. Alternative 2, Decentralized Management, was the highest cost alternative with a NPV of $1.3 billion. This option focuses on decentralizing program management to take advantage of existing organizational structures and reporting relationships. It is by far the highest cost option because this alternative would be far less efficient in bandwidth provision and software acquisition. Alternative 3 focuses on outsourcing the management of Global Network programs by shifting the responsibility for providing planning and execution to a contracting organization. The NPV of life-cycle costs for Alternative 3 is $807 million. This alternative's costs were higher than those of Alternative 1 due to higher software costs and initial planning, acquisition, and integration costs associated with outsourcing a major IT operation.

II.B. Risk Management

You should have performed a risk assessment during the early planning and initial concept phase of this investment's life-cycle, developed a risk-adjusted life-cycle cost estimate and a plan to eliminate, mitigate or manage risk, and be actively managing risk throughout the investment's life-cycle.

1. Does the investment have a Risk Management Plan?	Yes
a. If "yes," what is the date of the plan?	8/23/2004
b. Has the Risk Management Plan been significantly changed since last year's submission to OMB?	No

c. If "yes," describe any significant changes:

N/A

2. If there currently is no plan, will a plan be developed?	
a. If "yes," what is the planned completion date?	
b. If "no," what is the strategy for managing the risks?	

3. Briefly describe how investment risks are reflected in the life cycle cost estimate and investment schedule:

As part of the project management process, all Global Network projects identify and analyze risks during project planning. Risk analysis includes classifying the risks and assessing the risk probability, impact, immediacy, and controllability. These attributes help the Global Network program manager identify the greatest risks to the program and ensure they are appropriately mitigated. To facilitate risk analysis, all Global Network project managers (PMs) attended a risk assessment workshop. Using a risk assessment tool developed in concert with the Software Engineering Institute (SEI), the PMs answered a series of questions to more objectively quantify risk probability and impact, particularly related the project cost and schedule performance. The risk probability was then multiplied by the risk impact and incorporated into the cost and schedule estimates to account for risk. For example, a risk with an estimated $10,000 impact and 70% probability would cause the cost estimate to be increased by $7,000 ($10,000*70%). If a risk had an estimated two-month impact to the schedule and 50% probability, the schedule was increased by one month (2 months*50%). These schedule risks would also affect the cost estimates, since the cost of an additional month of work would need to be included. Although the original estimates were appropriately risk-adjusted, budget cuts have eliminated some of these adjustments and increased the program's cost risk. All projects within the Global Network follow the Managing State Projects (MSP) lifecycle and report on their risks at each control gate, in addition to semiannual project status reviews. Cost and schedule performance is tracked within the Earned Value Management System (EVMS), which has helped PMs understand how realized risks have affected the project - leading to better future estimates.